

**AFFIDAVIT OF UNITED STATES POSTAL INSPECTOR EDWARD PHILLIPS**  
**IN SUPPORT OF COMPLAINT**

I, EDWARD PHILLIPS, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I am a Postal Inspector with the U.S. Postal Inspection Service (“USPIS”) and have been in this role since July 2003. I am currently assigned to the Postal Inspection Service’s Mail Theft and Financial Crimes Task Force, which is comprised of personnel from the USPIS, Boston Police Department Special Investigation Unit, Homeland Security, State Department, Treasury Department, Secret Service and the Canton, Cambridge and Yarmouth Police Departments.

2. As a Postal Inspector with the Mail Theft and Financial Crimes Task Force, I have participated in numerous investigations relating to mail theft and financial crimes, including access device fraud and identity fraud. I have also participated in several narcotics investigations and have received specialized training regarding investigative techniques, evidence collection and evidence preservation.

**PURPOSE OF AFFIDAVIT**

3. This affidavit is being submitted in support of a criminal complaint against the following individuals:

A. Kevens Louis (“LOUIS”);



C. Lucson Appolon (“APPOLON”); and



(collectively, the “TARGET SUBJECTS”), charging that beginning at least in or about August 2018 and continuing until present, each did knowingly and willfully conspire with each other and

others unknown<sup>1</sup>, to perpetuate a fraudulent scheme through the abuse of the United States Postal Service's ("USPS") electronic Informed Delivery service in the Districts of Massachusetts, Maine, and New Hampshire, all in violation of Title 18, United States Code, Section 1349 (Conspiracy to Commit Wire Fraud) (the "TARGET OFFENSE").

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit does not purport to set forth all of my knowledge of, or investigation into, this matter. Rather, it sets forth only those facts that are necessary and sufficient to establish probable cause to believe that the TARGET SUBJECTS identified herein have committed the TARGET OFFENSE.<sup>2</sup>

5. I have participated in the below described investigation since August of 2018. I am familiar with the facts and circumstances of this investigation based on information I have received from a variety of sources, including my own personal participation in the investigation, oral and written reports made to me by other law enforcement officers, physical surveillance, public records and business records.

#### **BACKGROUND CONCERNING INFORMED DELIVERY**

6. Informed Delivery is a free electronic notification service provided by the USPS that gives residential and P.O. Box customers the ability to digitally preview their incoming letter-sized mail and manage their packages.<sup>3</sup>

---

<sup>1</sup> While USPIS' investigative efforts thus far have focused on the TARGET SUBJECTS, I am aware of other groups being pursued both locally and nationally for committing similar crimes. Investigation into other potential co-conspirators working with the TARGET SUBJECTS in furtherance of the TARGET OFFENSE is ongoing.

<sup>2</sup> The conduct also violates other federal offenses, including mail fraud (18 U.S.C. § 1341) wire fraud (18 U.S.C. § 1343), and identity theft (18 U.S.C. §§ 1028/1028A).

<sup>3</sup> Informed Delivery does not categorize mail based on which household member is the recipient. Therefore, an Informed Delivery account holder can also preview their spouse or children's mail.

7. In order to obtain an Informed Delivery account, potential users must first enter their address to confirm whether it is eligible. Assuming the address is eligible, potential users choose a username, password, security questions, and responses to those questions. Potential users also provide an email address and can choose to verify their identity by receiving an email or a letter at their physical residence. In some instances, potential users must also answer knowledge-based questions, which direct the respondent to verify personal details about themselves, such as prior addresses and their Social Security Number.

8. After the subscription is confirmed, Informed Delivery users can choose to log into their accounts to view incoming mail or can elect to receive emails containing images of the exterior address side of the incoming mail. The emails also include the mail's estimated arrival date.

**PROBABLE CAUSE TO BELIEVE THAT FEDERAL CRIMES WERE COMMITTED**

9. The investigation to date causes me to believe that from approximately August 2018 through at least January 2019, the TARGET SUBJECTS engaged in a conspiracy to commit wire fraud, in violation of Title 18 United States Code, Section 1349, through the use of Informed Delivery as set forth herein.

10. Based upon my training and experience, I believe the TARGET SUBJECTS access victims' personal identifying information, including names, Social Security Numbers, dates of birth, and addresses on the "dark web"<sup>4</sup> or on other forums, and then use the information to open credit cards in the victim's names.

11. The TARGET SUBJECTS then subscribe to Informed Delivery using the victims' personal identifying information and a fraudulent email address created by the TARGET

---

<sup>4</sup> The "dark web" is the portion of the Internet that is intentionally hidden from search engines and generally requires specific software, configurations, or authorization to access.

SUBJECTS for this purpose, in order to track the delivery of credit cards to the victims' residential mailboxes.

12. Generally, the TARGET SUBJECTS are careful to sign up for Informed Delivery accounts and credit cards using IP addresses that are not directly attributable to them, such as Wi-Fi at hotels and at public libraries. As set forth below however, in some instances the TARGET SUBJECTS inadvertently used IP addresses directly or indirectly attributable to them.

13. After signing up for Informed Delivery, the TARGET SUBJECTS sign up for credit cards in the same victim's names, and subsequently intercept the credit cards at the victims' mailboxes before the victims can receive them and use those credit cards at ATMs and to purchase gift cards and other items for resale at Apple and Walmart, among other retail establishments.

14. While the TARGET SUBJECTS are residents of Florida, they travel to other states, including Massachusetts and Maine to carry out the TARGET OFFENSE. The TARGET SUBJECTS generally target victims who live in wooded residential areas in relatively affluent suburbs with large lots and lengthy driveways to avoid detection by victim homeowners.

15. In August 2018, USPIS and local Massachusetts police departments began receiving mail theft and credit card fraud complaints in the Concord, Sherborn, Norfolk, and Weston areas. Victims reported that credit cards in their names were ordered without their knowledge and were then used at Apple and Walmart locations around the Boston, South Shore and Metro-west areas. Complaints from these Massachusetts towns continued through October 2018. Similarly, on or about December 24, 2018 through January 3, 2019, multiple victims from Kittery Point, Maine reported KeyBank credit cards that they had not ordered were used at Apple and Walmart locations in New Hampshire and Maine.

16. As set forth further below, video surveillance from Apple and Walmart reveal the victims' cards were used by individuals whose physical appearance matches the license

and social media photos of the TARGET SUBJECTS. IP information and electronic evidence gathered from the TARGET SUBJECTS personal Gmail accounts and from the fraudulent Informed Delivery accounts further underscores the TARGET SUBJECTS' involvement.

**I. Flight Record Information Obtained to Date Places the TARGET SUBJECTS in Boston and Maine**

17. Flight record information gathered to date<sup>5</sup> shows that the TARGET SUBJECTS frequently flew from Fort Lauderdale, Florida to Boston, and from Boston back to Fort Lauderdale during the relevant time period. For example, flight records show the following:

- a. APPOLON, [REDACTED] AND [REDACTED] flew from Fort Lauderdale to Boston on August 21, 2018 on Spirit on flight number NK610;
- b. LOUIS flew from Fort Lauderdale to Boston on August 22, 2018 on Spirit flight number NK610; and
- c. [REDACTED] flew from Fort Lauderdale to Boston on October 18, 2018 on Spirit flight number NK610 and from Boston to Fort Lauderdale on October 19, 2018 on spirit flight number NK615

18. Flight record information also places [REDACTED], LOUIS and [REDACTED] in Maine at the same time USPIS began receiving complaints of credit card fraud and mail theft.

Specifically, flight records show that on December 24, 2018, [REDACTED], LOUIS, and [REDACTED] flew from Fort Lauderdale to John F. Kennedy Airport ("JFK") in New York City, New York, on JetBlue flight number 002 and from JFK to Portland, Maine on JetBlue flight number 108.

On January 3, 2019, LOUIS flew from Boston to Jacksonville, Florida on JetBlue flight number 2009, and from Jacksonville to Fort Lauderdale on JetBlue flight number 1017.

**II. Rental Car Surveillance and Records Underscore the TARGET SUBJECTS' Involvement in the TARGET OFFENSE**

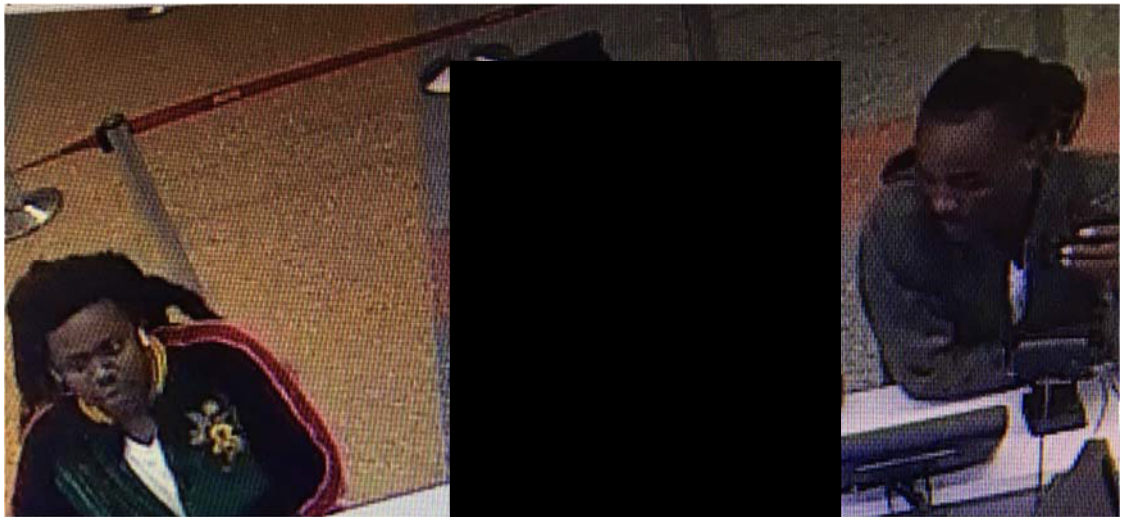
19. Rental car information and video surveillance further demonstrates that the

---

<sup>5</sup> This investigation is ongoing, and as such not all flight carriers have provided records at this time. Upon information and belief, the TARGET SUBJECTS utilized other carriers aside from JetBlue and Spirit Airlines ("Spirit"), and as such the below is intended to be only a representative example of the TARGET SUBJECTS flight patterns.

TARGET SUBJECTS rented vehicles in a manner consistent with the travel necessary to perpetuate the TARGET OFFENSE. On or about August 21, 2018, records show that [REDACTED] rented a Volvo XC6 from an Avis located at 15 Transportation Way, East Boston, Massachusetts 02128, bearing license plate NY JBC4439 (the “Volvo”)<sup>6</sup>. He returned the Volvo on or about September 19, 2018.

20. On September 19, 2018, video surveillance<sup>7</sup> depicts [REDACTED], APPOLON, and LOUIS renting a Chevy Traverse bearing New York license plate HZY5955 (the “Chevy Traverse”) from the same Avis location. Business records from Avis confirm that [REDACTED] was the signatory to the rental agreement.



21. On September 21, 2018, at approximately 3:08 p.m. (EDT), video surveillance from a trail camera installed by law enforcement captured the Chevy Traverse stopping in front of the mailbox at Victim 1’s house. Still footage reveals the hand of a black male<sup>8</sup> wearing a

---

<sup>6</sup> The Sherborn Police Department reported that on August 28, 2018, a Sherborn resident reported hearing his mailbox close as a vehicle matching the description of the Volvo sped away.

<sup>7</sup> In the Avis video footage, and as shown in the still image below, LOUIS is shown wearing a long sleeved green, red, and yellow sweat suit. LOUIS is shown wearing the same sweat suit in additional video footage obtained during this investigation, as noted *infra*, and in a video posted to his personal Instagram account on February 21, 2019.

garment with a black, white, and yellow sleeve reaching into the mailbox.



22. USPS records reveal that on September 10, 2018, the Target Subjects signed up for Informed Delivery using the name and address of Victim 1, a Weston, Massachusetts resident. The Target Subjects signed up for Informed Delivery using the email address love4boston508@gmail.com.<sup>9</sup>

23. Information obtained from local Massachusetts police departments demonstrates that during the time the Chevy Traverse was being used by the TARGET SUBJECTS, it was “queried” for suspicious activity around residential areas by officers in both Sherborn and Wellesley, Massachusetts.

### **III. Representative Transactions by Members of the Conspiracy**

24. While the parameters of the TARGET SUBJECTS’ various roles in the

---

<sup>8</sup>LOUIS is shown wearing a garment with the same sleeves in video footage obtained during this investigation. Specifically, LOUIS is shown on December 26, 2018 at Walmart in Scarborough, Maine using a victim’s KeyBank card (ending in 0884).

<sup>9</sup> Google is able to determine when one or more users log into multiple Gmail accounts from the same web browser through the use of “machine cookies,” which enable the end user to select a specific account from all those accessed from the same device. These shared cookies indicate that the same device accessed both accounts. As set forth in further detail below, the email address love4boston508@gmail.com is linked by machine cookies to vickyou6@gmail.com, an email address used by one or more of the TARGET SUBJECTS, including [REDACTED], to book flights in furtherance of the TARGET OFFENSE and to sign up for fraudulent Informed Delivery accounts and bank accounts.

conspiracy are not wholly defined at this stage of the investigation, each of the TARGET SUBJECTS appear to be involved in one or more of the critical steps in carrying out the conspiracy, namely in (1) creating fraudulent Informed Delivery accounts and opening bank accounts in victims' names, (2) physically retrieving the credit cards and other mail items from victim's mailboxes, and (3) using the victims' credit cards in fraudulent transactions. For example, [REDACTED] personal email address was used to sign up for numerous [REDACTED] Delivery and KeyBank Accounts, LOUIS's T-Mobile phone was used to access a KeyBank account opened in a victim's name, APPOLON's personal email address shares an IP address with logins to fraudulent Informed Delivery accounts and is linked to a fraudulent Informed Delivery account, and [REDACTED] rented the Volvo and Chevy queried by law enforcement.

25. Each of the TARGET SUBJECTS is repeatedly present on video surveillance, in most instances with one or more other members of the conspiracy, using the victims' credit cards at the same exact times bank records indicate the fraudulent transactions occurred. Notably, in some instances, the TARGET SUBJECTS attempt to disassociate with one another when entering or leaving Apple and Walmart, and cover their faces and/or heads, demonstrating they are aware of the illegality of their conduct.

26. In sum, the TARGET SUBJECTS engaged in dozens of fraudulent transactions between August 2018 and January 2019 with estimated losses of at least \$174,000 and exposure of over \$1.2 million. The transactions set forth below are representative examples only, which involve either electronic evidence, video evidence, or both.

A. [REDACTED]

i) [REDACTED] **Personal Email Address Is Used To Sign Up For Informed Delivery and KeyBank Accounts In Victims' Names**

27. Through open source data and social media websites, I determined that [REDACTED]



uses [REDACTED] as his personal email address and [REDACTED] as the recovery email address<sup>10</sup> for [REDACTED]

28. Although in most instances, the TARGET SUBJECTS operated covertly, utilizing newly created email accounts to sign up for fraudulent Informed Delivery accounts, on several occasions, one or more of the TARGET SUBJECTS used [REDACTED] personal email addresses to sign up for Informed Delivery and KeyBank credit cards in third-party victims' names.<sup>11</sup>

**ii) The Fraudulent Email Account vickyou6@gmail.com Contains Airline Tickets and Other Receipts Directly Attributable to [REDACTED]**

29. The email address vickyou6@gmail.com, referenced in footnote 7 and *infra* is also directly tied to [REDACTED]

30. A search warrant return for vickyou6@gmail.com shows that the email account was used almost solely in furtherance of the TARGET OFFENSE. The account contains photographs of victim information and mail items, and a screenshot of a fraudulent Santander bank signup that one or more of the TARGET SUBJECTS sent to [REDACTED] at trymeagain93@yahoo.com. It also contains numerous items directly attributable to [REDACTED], including airline tickets to/from Boston and emails from the Seminole Casino addressed to him.

**iii) [REDACTED] and APPOLON Use Victim 2's Credit Card at Apple**

31. On or about August 16, 2018, one or more of the TARGET SUBJECTS signed up for a KeyBank card using the name, Social Security Number, date of birth, and address of Victim

---

<sup>10</sup> By its nature, account recovery information is provided by the account holder as a means to ensure the account holder can still access his or her account in the event of a stolen or forgotten password. Necessarily, account recovery information must also belong to or be controlled by the account holder, otherwise the account holder could not utilize the recovery account as an alternative method to gain access to his/her account.

<sup>11</sup> For example, on August 18, 2018, one or more of the TARGET SUBJECTS used trymeagain93@yahoo.com to sign up for a KeyBank account using the name, Social Security Number, date of birth, and address of a victim in Massachusetts. On September 13, 2018, one or more of the TARGET SUBJECTS used pjean108@yahoo.com to sign up for at least three Informed Delivery accounts at addresses in Massachusetts. On the same date, one or more of the TARGET SUBJECTS used the same email address to sign up for two KeyBank accounts using the name, Social Security Number, date of birth, and address of two additional victims in Massachusetts.

2, a Sherborn, Massachusetts resident, and the email address vicky6@gmail.com.

32. Bank records and Apple surveillance shows that on August 24, 2018 at approximately 5:43 p.m. (EDT) [REDACTED] and APPOLON entered the Apple Store at 815 Boylston Street, Boston, Massachusetts 02467 and used a KeyBank credit card registered in Victim 2's name (ending in 7916) to purchase an Apple iPhone X.

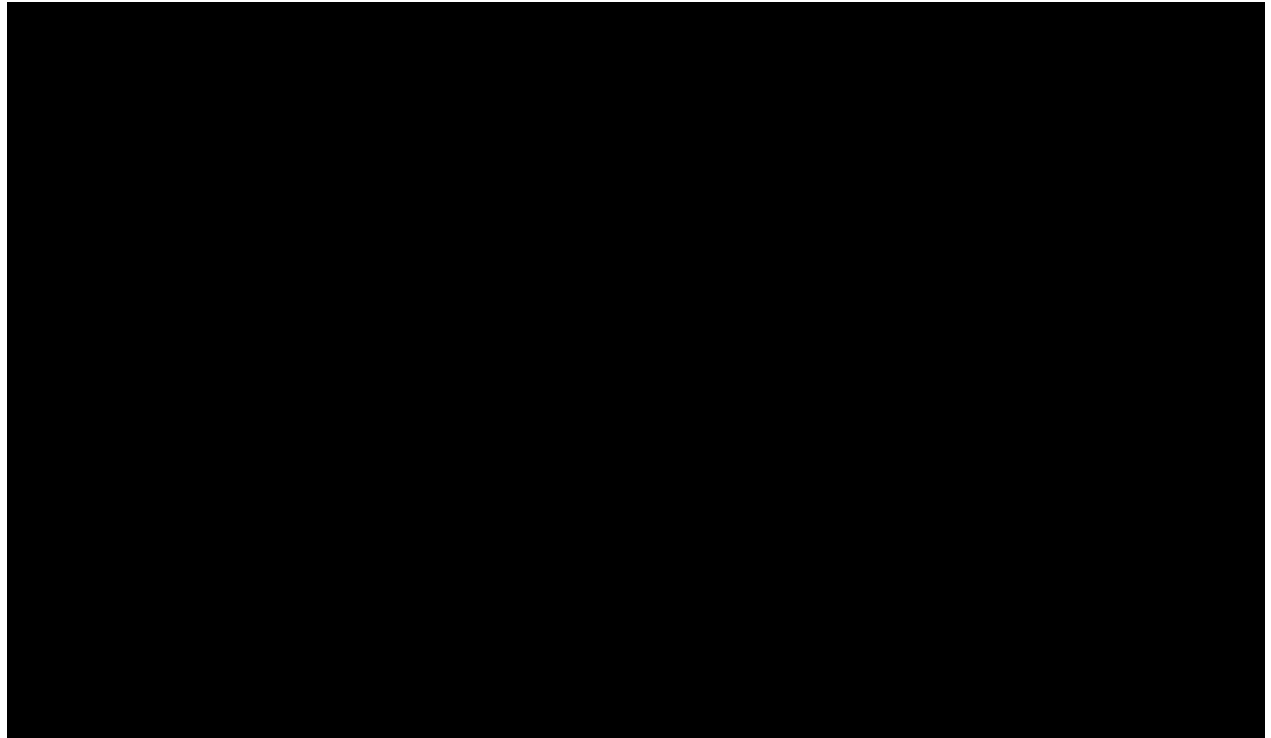
33. On August 25, 2018, bank records demonstrate Victim 2's credit card was used again to purchase four Apple iPhone X's at the same Apple store.

**iv) [REDACTED] and [REDACTED] Use Victim 3's Credit Card at Walmart and Apple**

34. On December 15, 2018, one or more of the TARGET SUBJECTS signed up for a KeyBank card using the name, Social Security Number, date of birth, and address of Victim 3, a Kittery, Maine resident, and the email address innocent20151@gmail.com.

35. Bank records and Walmart video surveillance show that on December 26, 2018, [REDACTED] and [REDACTED] used a KeyBank credit card registered in Victim 3's name (ending in 3034) to purchase seven gift cards and a mobile phone at the Walmart located at 30 Landing Road, Windham, Maine 04062.

36. Bank records and Apple video surveillance show that on December 29, 2018, at approximately 7:30 p.m. (EST) [REDACTED] and [REDACTED] used a KeyBank card issued in a fictitious name, linked to the KeyBank account registered in Victim 3's name, to purchase four iPhone Xs and urBeats3 wired earphones at the Apple Store located at The Mall of New Hampshire, 1500 S. Willow Street, Manchester, New Hampshire 03103. In this video, [REDACTED] is wearing a knit Chicago Bulls hat. [REDACTED] is depicted wearing the same exact hat in a March 19, 2017 photograph on his social media account, in posts on LOUIS' social media account dated March 19, 2017, March 20, 2017, March 24, 2017 and April 2, 2017, and in additional video surveillance obtained during this investigation, as referenced *infra* in paragraph 72.



**B. KEVENS LOUIS**

**i) LOUIS and [REDACTED] Use Victim 4's Credit Card at Apple**

37. On or about August 16, 2018, one or more of the TARGET SUBJECTS signed up for a KeyBank card using the name, Social Security Number, date of birth, and address of Victim 4, a Sherborn, Massachusetts resident, using the email address loveorhate20151@gmail.com.

38. On August 17, 2018, one or more of the TARGET SUBJECTS signed up for Informed Delivery using the name and address of Victim 4 and the email address lifegoeson20181@gmail.com.

39. On August 29, 2018, at approximately 1:21 p.m. (EDT) LOUIS and [REDACTED] entered the Apple Store at Solomon Pond Mall, 601 Donald Lynch Boulevard, Marlborough, Massachusetts 01752. Bank records and Apple surveillance show LOUIS and [REDACTED] using a credit card registered in Victim 4's name (ending in 2504) to purchase 4 Apple iPhone X's and one set of air pods. LOUIS is shown wearing the same sweat suit referenced in footnote 7, *supra*. [REDACTED] is shown wearing the Chicago Bulls hat, and a red tee shirt that has the words

“ALL ABOUT THE MULA” written on it in white capital letters, as shown below:



- ii) LOUIS, [REDACTED] and [REDACTED] Use Victim 5 and Victim 6's Credit Cards at Walmart, and Victim 5's Fraudulent KeyBank Account is Accessed By LOUIS on his T-Mobile Phone

40. On or about September 12, 2018, one or more of the TARGET SUBJECTS signed up for a KeyBank credit card using the name, Social Security Number, date of birth, and address of Victim 5, a Norfolk, Massachusetts resident, and the email julianneflightagent@gmail.com.

41. On or about September 12, 2018, one or more of the TARGET SUBJECTS signed up for Informed Delivery and created two different accounts using the name and address of Victim 5, and the email addresses nozoeftbehind123@gmail.com<sup>12</sup> and saccone123

---

<sup>12</sup> Upon information and belief, the phrase “nozoeftbehind” is a reference to Zoe Pound, a Miami-based gang whose criminal activities include drug trafficking, extortion, home invasion, human smuggling, money laundering,

@gmail.com.

42. On or about September 16, 2018, one or more of the TARGET SUBJECTS accessed the julianneflightagent@gmail.com account using the IP address<sup>13</sup> 2607:fb90:689d:a506:8851:227b:6d3c:13d7 (“IP Address #1”).

43. Using open source materials, I confirmed that the IP Address #1 belongs to T-Mobile. T-Mobile records show that IP Address #1 was assigned<sup>14</sup> to subscriber LOUIS.

44. On September 18, 2018, at approximately 6:00 p.m. (EDT), video surveillance depicts LOUIS, [REDACTED] and [REDACTED], entering Walmart located at 66 Parkhurst Rd., Chelmsford, Massachusetts 01824. Bank records and Walmart video surveillance shows LOUIS, [REDACTED], and [REDACTED] using a KeyBank credit card registered in Victim 5’s name (ending in 3561) and a KeyBank credit card registered in the name of Victim 6, a Weston, Massachusetts resident, (ending in 2082) to purchase approximately \$4,800 worth of gift cards. Notably, LOUIS is shown wearing the same sweat suit referenced in footnote 6, *supra*, and [REDACTED] is again shown wearing the same Chicago Bulls hat.

**iii) LOUIS and [REDACTED] Use Victim 7’s Credit Card at Walmart**

45. On or about September 8, 2018, one or more of the TARGET SUBJECTS signed up for a KeyBank credit card using the name, Social Security Number, date of birth, and address of Victim 7, a Concord, Massachusetts resident, and the email address bostonteam2020@gmail.com.

---

and racketeering. LOUIS’ Instagram account repeatedly uses the hashtag #nozoeleftbehind. Additionally, USPIIS has discovered numerous other fraudulent Informed Delivery accounts created using email addresses with the same phrase “nozoeleftbehind” with various numbers added at the end.

<sup>13</sup> On or about September 17, 2018, one or more of the TARGET SUBJECTS logged into a fraudulent Informed Delivery account created on September 16, 2018, using the email address jugseason1804@gmail.com via IP Address #1.

<sup>14</sup> LOUIS has since closed this account.

46. The recovery email address for bostonteam2020@gmail.com is rjohnson33@ymail.com. On or about August 27, 2018, the credit card of Victim 2 was used to pay for a five-night stay at the Days Inn in Shrewsbury, Massachusetts. The name provided to the Days Inn in conjunction with the reservation was “Robert Johnson”. A copy of “Robert Johnson’s” Florida license depicts an individual who appears to be [REDACTED]

47. Google subpoena returns reveal that one or more of the TARGET SUBJECTS logged into bostonteam2020@gmail.com on September 8, 2018, via the IP address 96.92.158.209, (“IP Address #2”). IP Address #2 was also used to log into APPOLON’S personal email address, youngaj62@gmail.com, on September 14, 2018 and the following email addresses between September 7 and September 12, 2018 (all of which were used in connection with fraudulent Informed Delivery signups in Massachusetts): love4boston508 @gmail.com, mariapineda20150@gmail.com, nancymoore617@gmail.com<sup>15</sup>, and vickyou6@gmail.com. IP Address #2 is assigned via Comcast to a Motel 6 located at 1668 Worcester Rd, Framingham, Massachusetts 01762.<sup>16</sup>

48. On September 19, 2018 at approximately 4:57 p.m. (EDT), video surveillance depicts LOUIS and [REDACTED] entering Walmart at 200 Otis Street, Northborough, Massachusetts 01532. Bank records and Walmart video surveillance show LOUIS and [REDACTED] using a KeyBank credit card registered in Victim 7’s name (ending in 6034) to purchase approximately \$3,197.22 of gift cards, a mobile phone and men’s clothing.

### **C. LUCSON APPOLON**

---

<sup>15</sup> As set forth *infra*, nancymoore617@gmail.com is also linked to APPOLON’s personal email account via machine cookies.

<sup>16</sup> At this stage of the investigation, I believe that the TARGET SUBJECTS were staying at this hotel using fake identification documents. While I am aware the TARGET SUBJECTS used the alias Robert Johnson (at Days Inn) and Penny Fasel (at a La Quinta Inn), it has not yet been determined what identity the TARGET SUBJECTS were using at the Motel 6.

**i) APPOLON'S Personal Email Account Shares IP Address With Fraudulent Informed Delivery Accounts and Is Linked By Cookies to Fraudulent Informed Delivery Account**

49. Account logins for APPOLON's personal email addresses match IP logins for fraudulent Informed Delivery signups and share machine cookies with a fraudulent Informed Delivery account.

50. Through open source information, flight records<sup>17</sup>, and social media accounts, I determined that APPOLON uses youngaj62@gmail.com as his personal email address and rorolone@yahoo.com, as a recovery email address for youngaj62@gmail.com, evidencing that he has access to both email accounts.

51. The IP address 68.114.85.32 ("IP Address #3") is linked to both fraudulent Informed Delivery signups<sup>18</sup> on September 15, and September 16, 2018 and to account logins for youngaj62@gmail.com and rorolone@yahoo.com on September 16, 2018.

52. IP Address #3 belongs to a Super 8 Motel<sup>19</sup> in Sturbridge, Massachusetts.

**ii) APPOLON Uses Victim 8's Credit Card at Walmart**

53. On or about September 7, 2018, one or more of the TARGET SUBJECTS used the name, Social Security Number, date of birth, and address of Victim 8, a Concord, Massachusetts resident, to sign up for a fraudulent KeyBank account using the email address mariapineda20150@gmail.com.<sup>20</sup>

---

<sup>17</sup> APPOLON provided the same email address to Spirit in connection with his September 26, 2018 flight.

<sup>18</sup> The four Informed Delivery accounts that were set up using the IP Address #3 used the email addresses youboy5090@gmail.com, jugseason1804@gmail.com, vicky06@gmail.com, and playerhard@yopmail.com and pertained to victim addresses in Concord and Weston, Massachusetts. As set forth in paragraph 42 *supra*, jugseason1804@gmail.com was accessed via IP Address #1, assigned to LOUIS.

<sup>19</sup> At this stage of the investigation, I believe that the TARGET SUBJECTS were staying at this hotel using fake identification documents. It has not yet been determined what identity the TARGET SUBJECTS were using.

<sup>20</sup> IP Address #2, used to log into APPOLON's personal Gmail account on September 14, 2018, was also used to log into mariapineda20150@gmail.com on September 7, 2018, as set forth *supra* in paragraph 47.

54. On or about September 15, 2018 one or more of the TARGET SUBJECTS used Victim 8's name and address to sign up for a fraudulent Informed Delivery accounts using the email address livelife20181@gmail.com.

55. On September 16, 2018, at approximately 3:30 p.m. (EDT) APPOLON and [REDACTED] entered Walmart located at 25 Tobias Boland Way, Worcester, Massachusetts 01607. Walmart video surveillance depicts APPOLON and [REDACTED] using a KeyBank credit card registered in Victim 8's name (ending in 2934) to purchase six Visa prepaid gift cards.

**iii) APPOLON Uses Victim 9's Credit Card at Santander ATM**

56. On or about September 12, 2018, one or more of the TARGET SUBJECTS used Victim 9's name, Social Security Number, date of birth, and address to sign up for a fraudulent Santander account using the email address nancymoore617@gmail.com. APPOLON's personal email account, youngaj62@gmail.com is linked by cookies to nancymoore617@gmail.com, meaning the same individual signed into the two accounts using the same device.

57. On September 13, 2018, one or more of the TARGET SUBJECTS signed up for a fraudulent Informed Delivery account with Victim 9's name and address, again using the email address nancymoore617@gmail.com.

58. On September 18, 2018 at approximately 9:20 p.m. (EDT), Santander video surveillance depicts APPOLON using a Santander card registered in Victim 9's name (ending in 0541) to withdraw approximately \$500 from the Santander ATM located at 379 Main Street, Sturbridge, Massachusetts 01566.

**D. [REDACTED]**

**i) [REDACTED] Uses Victim 10's Credit Card at Santander ATM**

59. On September 10, 2018, one or more of the TARGET SUBJECTS used the name, Social Security Number, date of birth, and address of Victim 10, a resident of Concord,



Massachusetts to sign up for a fraudulent Santander account using the email address keyislife23@gmail.com.

60. On September 11, 2018, one or more of the TARGET SUBJECTS used the same information to sign Victim 10 up for a second Santander credit card, again using the email address keyislife23@gmail.com.

61. On the same date, one or more of the TARGET SUBJECTS signed up for an Informed Delivery account using Victim 10's name and address and the email address magic4good44+mike@gmail.com.<sup>21</sup>

62. On September 17, 2018 at approximately 9:15 p.m. (EDT), Santander video surveillance depicts [REDACTED] attempting to use a Santander card registered in Victim 10's name (ending in 6249) to withdraw funds from the Santander ATM located at 6 Francis Street, Boston, Massachusetts 02115.

63. In the video, [REDACTED] is again wearing the same Chicago Bulls hat and the same "ALL ABOUT THE MULA" tee shirt.

**ii) [REDACTED] uses Victim 11's Credit Card at Santander ATM**

64. On September 18, 2018, at approximately 7:00 p.m. (EDT), Santander video surveillance again shows [REDACTED], accompanied by APPOLON, using a Santander card registered in Victim 11's name (ending in 9661) to withdraw approximately \$500 from the Santander ATM located at 1 Wood St., Lowell, Massachusetts 01851. [REDACTED] is wearing the same Chicago Bulls hat in the video.

**iii) [REDACTED] uses Victim 12's Credit Cards in Maine and in Florida**

65. On December 14, 2018, one or more of the TARGET SUBJECTS used the name,

---

<sup>21</sup> Notably, the Informed Delivery username one or more of the TARGET SUBJECTS chose was keylife2016.

Social Security Number, date of birth, and address of Victim 12, a resident of Kittery, Maine to sign up for a fraudulent KeyBank account, using the email address oldfart19291@yahoo.com.

66. On December 16, 2018, one or more of the TARGET SUBJECTS signed up for a fraudulent Informed Delivery account using Victim 12's name and address, and the email schroeder19551@gmail.com.

67. On December 26, 2018, at approximately 4:40 p.m. (EST) [REDACTED] and [REDACTED] entered Apple at Maine Mall, 364 Maine Mall Rd Suite E107, South Portland, Maine 04106 and used a KeyBank credit card registered in Victim 12's name (ending in 9684) to purchase four Apple iPhone X's and a silicone case.

68. On December 28, 2018, video footage and bank records show [REDACTED] using Victim 12's KeyBank card again, this time to purchase four VISA prepaid cards at the Walmart, 500 Gallery Blvd., Scarborough, Maine 04074.

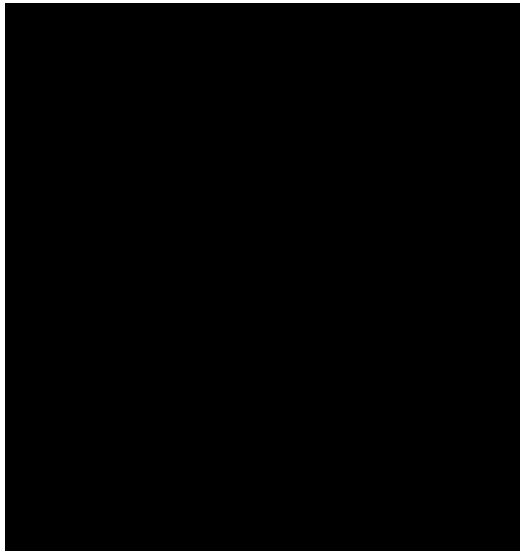
69. On or about December 27, 2018, one or more of the TARGET SUBJECTS used the name, Social Security Number, date of birth, and address of Victim 12, to sign up for a fraudulent Bank of America account (the "BOA Account").

70. On or about December 27, 2018, a client of Victim 12's wrote him a check for \$1400 as payment for Victim 12's consulting services. When Victim 12 did not receive the check, he called the client who informed him that the check had already been deposited.

71. Records and video surveillance from Bank of America show that on or about January 8, 2019, [REDACTED] deposited the check for \$1400 into the BOA Account at a Bank of America ATM located in the Maine Mall, South Portland, Maine 04106.

72. On January 12, 2019, video footage from a Bank of America ATM in Lauderhill, Florida shows [REDACTED], withdrawing \$200 from the BOA Account. In the video, [REDACTED] is again wearing the same Chicago Bulls knit hat and is attempting to cover his face with his

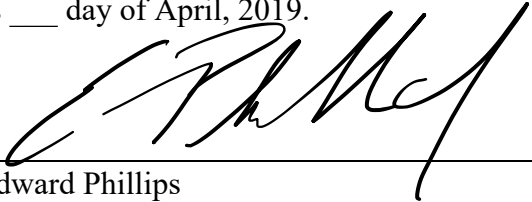
iPhone.



**CONCLUSION**

Based upon the foregoing, I have probable cause to believe that LOUIS, [REDACTED] APPOLON, and [REDACTED] have committed the crime of conspiracy to commit wire fraud, in violation of Title 18 United States Code, Section 1349.

Sworn to under the pains and penalties of perjury, this 9th day of April, 2019.

  
\_\_\_\_\_  
Edward Phillips  
Postal Inspector  
United States Postal Inspection Service

Subscribed and sworn to before me  
on April 8, 2019

  
\_\_\_\_\_  
UNITED STATES MAGISTRATE JUDGE

